Homeless Management Information System
Policies and Standard Operating Procedures

January 15, 2014

CoC Board – Approved March 27, 2014

Table of Contents

History of the HMIS in Indiana

In 2004, the US Department of Housing and Urban Development ("HUD") published the Homeless Management Information Systems; Data and Technical Standards Final Notice for Homeless Management Information Systems ("HMIS"). These standards defined the data elements and formats through which all HUD McKinney-Vento Program funded projects were to report. In Indiana, a statewide coalition consisting of homeless providers and local Continuums of Care was established to review and select a software vendor for the Indiana Balance of State HMIS. After review, the Affordable Wide Area Relational Data System ("AWARDS") from Foothold Technology, Inc. was selected. This was a web-based software requiring only Internet access for use. The HMIS was initially separately administered for South Bend, Evansville and the Indiana Balance of State (89 of the 92 counties in Indiana) by the Indiana Coalition on Housing and Homeless Issues ("ICHHI"), a non-profit agency.

Since then, HMIS usage in the state has grown, with the responsibility for actual management of the effort transferring to the Indiana Housing and Community Development Authority ("IHCDA") in March of 2009. In 2009, the HMIS efforts in the Balance of State for Indiana was supported by three (3) HUD grants to IHCDA, Evansville and South Bend. At that time Foothold was utilized for HMIS. Then HUD provided guidance that indicated that there could not be more than one (1) lead HMIS agency per Continuum of Care "CoC", and IHCDA became the lead agency for the Balance of State. In 2010, IHCDA decided to transfer from Foothold Technology, Inc. to ClientTrack, Inc. ("ClientTrack") formerly known as Data Systems International for the State's HMIS needs. In 2011, IHCDA contracted with Client Track to provide the HMIS software. The focus of this effort was to expand participation in HMIS by homeless service providers. In 2013, IHCDA anticipates providing a closed database that is comparable to HMIS database to victim service providers. IHCDA allows agencies that are located in the Indiana Balance of State and provide services to the homeless to participate in the HMIS and the closed system at no charge. IHCDA employs staff whose primary job responsibilities are devoted to the expansion, training and maintenance of the HMIS in Indiana. IHCDA staff is involved in the following activities: operating the online help desk, providing various types of user training, supporting the local Continuums of Care, preparing the annual Point in Time Count data, developing the Annual Homeless Assessment Report (AHAR) and assisting in evaluating HUD McKinney-Vento applicants. The responsibility for the overall oversight of the HMIS effort rests with the IHCDA Board of Directors, which delegated it to the CoC Board, which oversees the Data Collection and Evaluation Committee. The Data Collection and Evaluation Committee includes representatives from State agencies, academia, homeless service providers, users of the HMIS, and advocates for the homeless.

The Data Collection and Evaluation Committee periodically reviews user and executive satisfaction with the present software, discusses changes in data standards required by HUD and opportunities to improve the system, especially with respect to increasing its use by non-HUD funded homeless providers. The goal for the HMIS is its statewide adoption by over seventy-percent (70%) of all homeless providers and eighty-five percent (85%) of all transitional and permanent supportive housing providers.

The HMIS database is hosted by IHCDA and is operated in secure environment which requires a personally assigned log-in password to access. Each HMIS user must complete a User Agreement/Code of Ethics, which confirms the User's responsibility to protect the client's Protected Personal Information ("PPI"). Each new HMIS user must complete training. Security and privacy training is also provided to new users and performed annually, thereafter. The Agency will only allow staff members, who need information from the HMIS for legitimate business purposes to be provided log in access to the HMIS. Additionally, each agency that participates in the HMIS must complete an HMIS Participation

Agreement, which confirms the Agency's privacy standards and computer safeguards required to be used by the Agency while using the HMIS and the information being entered into HMIS. Data integrity is assured by several levels of backup, including a separate annual archive.

Purpose of HMIS Policies and Standard Operating Procedures

The purpose of these HMIS Policies and Standard Operating Procedures ("Policies and Standard Operating Procedures") is to provide guidelines, requirements, responsibilities, processes, and procedures governing the operation of the HMIS, with an emphasis on protecting the privacy of Clients and the security of Client information. These Policies and Standard Operating Procedures apply to IHCDA and HMIS Staff, Agencies, Agency Users, the HMIS Software Vendor, and any other entity involved in the administration of HMIS.

Definitions for HMIS Policies and Standard Operating Procedures

Definitions:	The following definitions shall be applicable for the HMIS Policies and Standard Operating Procedures.

Agency: An organization working with IHCDA signing an Agency Partner Agreement thereby agreeing to follow HMIS Policies and Standard Operating Procedures. The Agency Partner Agreement is in effect for all related programs within an Agency.

Agency Executive User: The individual at an Agency who is the chief liaison between IHCDA and the Agency and whose responsibilities are more fully described in the "Agency Participation Requirements" Policy and Standard Operating Procedure.

Agency User or User: An employee, agent, or other representative authorized by an Agency to receive an HMIS username and password.

Aggregated Data: This is data that is grouped, usually by program, but possibly across any dimension (e.g., time, county sub region, segments of Client populations, etc.). This data type precludes exploration at a Client-identified level because all Client-level information is de-identified.

Client: A person who applies for or receives services from an Agency.

Client-level Information: A set of data records that combined represent a single Client. This type of information lends itself to more in-depth data analysis. All public Client-level Information is De-identified Information.

De-identified Information: A data set or report that removes all Protected Personal Information, (*i.e.*, information that identifies the Client by name, SSN or other unique identifier).

Disclosure: The release, transfer, or provision of access to information outside the HMIS.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et. seq., and its implementing regulations (all as amended).

HMIS: Homeless Management Information System — a web based computer system managed by IHCDA staff that collects Client- identifying Confidential Information with services received and outcomes achieved by the Clients.

HMIS Staff: IHCDA employees and/or contractors involved in administering the HMIS.

HMIS Software Vendor: ClientTrack, Inc.

Institutional Review Board (IRB): A committee of individuals that ascertains and approves the acceptability of proposed Research and the use of Clients and Protected Personal Information in terms of institutional commitments and regulations, applicable law, and standards of professional conduct and practice.

Minimum Necessary: The minimum amount of Protected Personal Information needed to accomplish the purpose of a request or to assess Client eligibility to provide services to the Client.

Protected Personal Information: Any information maintained by an Agency or in HMIS about a Client or homeless individual that: (i) identifies, either directly or indirectly, a specific individual; (ii) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (iii) can be linked with other available information to identify a specific individual. The term shall include Protected Health Information. This information may include demographic or financial information about a particular Client that is obtained through one or more sources. This may include information such as name, address, social security number, income, education and housing information.

Protected Health Information: Any individually identifiable information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

Program Specific Data Elements: Additional data elements that are specific to the services provided by the Agency to each Client. Program Data are a mix of those elements required to complete the HUD APR (Annual Progress Report) and additional elements suggested by other federal agencies, HMIS practitioners and researchers.

Public Data: De-identified Information approved for release to external parties and the public. It may be either Client-level Information or Aggregated Data.

Research: An activity is defined as research when it meets the following definition: "a systematic investigation, including Research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of Research repositories and databases for Research." *(45 CFR, Part 46 — The Common Rule).* For purposes of this Policy, any use of Protected Personal Information for Research purposes must be for academic Research conducted by an individual or institution that has a formal relationship with IHCDA if the Research is conducted either: (1) by an individual employed by or affiliated with IHCDA for use in a research project conducted under a written research agreement approved in writing by the RARC; or (2) by an institution for use in a research project conducted under a written research agreement approved in writing by the RARC.

Stakeholders: IHCDA sponsors, participating agencies, programs, and homeless persons.

Universal Data Elements: Basic demographic data elements defined in the HUD Data Standards including those the Agency staff are responsible for entering into the HMIS:

Name	Veteran Status	Program entry date	Social Security Number
Date of Birth	Prior Residence	Program exit date	Zip Code last permanent address
Gender	Ethnicity & Race	Disabling Condition	Destination
Personal identification number	Household number	Head of household	Length of time on street, emergency shelter or safe haven

Agency Participation Requirements

Policy:	IHCDA will establish requirements for agencies that participate in the HMIS. All requirements for participation are outlined in the sections below. To date, participation is limited to agencies engaged in providing services to the homeless, including PATH teams.

Procedure:

A. IDENTIFICATION OF AGENCY EXECUTIVE USER:

Each Agency must identify an individual who will serve as its Agency Executive User. Agency Executive Users for the HMIS play a critical role in the protecting HMIS data. Some agencies in the Regional Planning Councils have Information Technology Department Staff who could also serve as an Agency Executive User. Time, interest, and ability are the biggest factors in determining who should be an Agency Executive User for the HMIS. This title does not necessarily correspond to the Agency's organizational chart. The Agency User designated as the Agency Executive User may also be a staff member who enters Client data. The Agency Executive User must attend training provided by IHCDA prior to performing the role. Roles and responsibilities for the HMIS Agency Executive Users include the following:

1. Determining appropriate access to the HMIS for each Agency User. This determination should be based on each Agency User's job function as it will relate to the HMIS data entry and retrieval (*i.e.*, role based security).
2. Detecting and responding to violations of HMIS policies or Agency policies and procedures.
3. Developing strict procedures for issuing, altering and revoking HMIS access privileges.
4. Ensuring system auditing (within the Agency).
5. Ensuring Agency-wide data quality.
6. Ensuring the security of the HMIS on the Agency website.

7. Notifying IHCDA staff of any security breach within twenty-four (24) hours of the breach.

8. Enforcing Agency information system policies and standards.

B. IDENTIFICATION OF SECURITY OFFICER:

It would be beneficial for the Agency to assign a HMIS security officer who will be responsible for ensuring compliance with the applicable security standards. The Agency should designate in writing, the individual that has been appointed to serve in this role. Each HMIS security officer should receive HMIS training. The security officer must pass a criminal background check.

C. TRAINING:

Agency Executive Users and Agency Users must attend training(s) prior to accessing the HMIS. If the Agency Executive User for the Agency changes, then the new Agency Executive must attend training conducted by IHCDA Staff or by an individual approved by IHCDA. All new Agency Users of the HMIS must undergo formal training provided by IHCDA Staff or an individual authorized by IHCDA. The Agency Executive User and Agency Users will attend follow-up training regarding data quality and completeness. Security training must be provided to each Agency User, prior to the User being given access to HMIS and annually thereafter. All users of HMIS must complete a criminal background check prior to using HMIS.

D. PRIVACY PRACTICES:

The **HMIS Privacy Practices Notice** provides information to Clients about why the Agency collects personal information from them and refers them to **HMIS Notice of Privacy Practices** for additional information regarding how this information may be used or disclosed. The current **HMIS Privacy Practices Notice and HMIS Statement of Privacy Practices** both will be posted at www.in.gov/myihcda/2444.htm.

The **HMIS Privacy Practices Notice** must be posted at each intake location and on the Agency's website, if applicable, to ensure that the Client is informed of why the information is being collected and privacy protections that the Agency will utilize to protect its information. The Agency Executive User will ensure that privacy and security training is provided to each Agency User, annually. If the Agency is a "covered entity" under the Health Insurance Portability and Accountability Act of 1996, it may combine the **HMIS Statement of Privacy Practices** with the notice of privacy practices required by HIPAA. Agencies must request IHCDA to review any such combined Notice of Privacy Practices for compliance with HMIS and IHCDA standards. The Agency's privacy practices must meet the following requirements:

1. Collection Limitation: An Agency may collect Protected Personal Information ("PPI") only when appropriate to the purposes for which the information is obtained or when required by law. An Agency must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the Client. An Agency must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. Consent of the individual for data collection may be inferred from the circumstances of the collection. An Agency should use the following language to meet this standard: "We collect personal information directly from you for reasons that

are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for our clients, and to better understand the needs of our clients. We only collect information that we consider to be appropriate."

2. Data Quality: PPI collected by an Agency must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely. In consultation with IHCDA, an agency must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PPI that is not in current use seven (7) years after the PPI was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

3. Purpose Specification and Use Limitation: An Agency may only use the PPI in accordance with the **HMIS Privacy Practices Notice**. An Agency may use or disclose PPI only if the use or disclosure is allowed by the **HMIS Statement of Privacy Practices**. An Agency may infer consent for all uses and disclosures specified in the notice and for uses and disclosures determined by the Agency to be compatible with those specified in the notice. Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the **HMIS Statement of Privacy Practices** can be made only with the consent of the individual or when required by law.

4. Openness: An Agency must publish the **HMIS Statement of Privacy Practices** describing its policies and practices for the processing of PPI and must provide a copy of the **HMIS Statement of Privacy Practices** to any individual upon request. If an Agency maintains a public web page, the Agency must post the current version of the **HMIS Statement of Privacy Practices** on the web page. An Agency may, if appropriate, omit its street address from the **HMIS Statement of Privacy Practices**. An Agency must post a sign stating the availability of the **HMIS Statement of Privacy Practices** to any individual who requests a copy. An Agency must state in the **HMIS Statement of Privacy Practices** that the policy may be amended at any time and that amendments may affect information obtained by the Agency before the date of the change. An amendment to the **HMIS Statement of Privacy Practices** regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

5. Access and Correction: In general, an Agency must allow an individual to inspect and to have a copy of any PPI about the individual. An Agency must offer to explain any information that the individual may not understand.

   An Agency must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. An Agency is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information. In accordance with the **HMIS Statement of Privacy Practices**, an Agency may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PPI:

   a. Information compiled in reasonable anticipation of litigation or comparable proceedings;

b. Information about another individual (other than a health care or homeless provider);

c. Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or

d. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

An Agency can reject repeated or harassing requests for access or correction. An Agency that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Prior to agreeing to grant an individual a right to access or correct their records, an Agency shall consult with IHCDA to ensure that the proper coordination between the Agency's response and the capabilities of the HMIS system will occur, unless the requested correction is a routine correction of a common data element for which a field exists in HMIS (*e.g.*, date of birth, prior residence, social security number, etc.).

6. Accountability: An Agency must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. Each Agency shall forward any complaints regarding the use or disclosure of Client information by or through the HMIS for IHCDA's evaluation of the complaint. An Agency must require each member of its staff who utilize HMIS (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) the **HMIS User Agreement/ Code of Ethics** that acknowledges receipt of a copy of the **HMIS Statement of Privacy Practices** and that pledges to comply with the **HMIS Statement of Privacy Practices**.

7. **Additional Privacy Considerations:**

8. No agency will sell or lease or give away PPI that is collected and will not share PPI from Agency Users without first informing them that information will be collected or shared, and with whom it might be shared. Log Files: We may use IP addresses to analyze trends, administer the site and gather broad demographic information for aggregate use. IP addresses are not linked to PPI.

E. CLIENT CONSENT FORMS:

The HMIS allows implied consent for the collection of Client information by prominently posting the **HMIS Privacy Practices Notice**. The HMIS also allows for disclosure of Client information in strict accordance with the **HMIS Statement of Privacy Practices**. Nevertheless, Client has the right to place limitations on the sharing of his or her PPI.

F. CLIENT RIGHTS

1. Grievance

a. Each Client has the right to ask questions and submit complaints about the Agency's privacy and security policies and appeal determinations made by the Agency in accordance with the Agency's established grievance policy.

b. Complaints about the conduct or practice of the Agency and its handling of PPI may be filed in writing to the IHCDA's Compliance Attorney.

c. Agencies are responsible for establishing an internal grievance process to handle Client complaints and grievances related to consent and release of information related to the HMIS system. If a Client has a grievance regarding erroneous data entry or inappropriate use of their data, the Client will need to follow the Agency's established guidelines, standard operating procedures or protocol on resolving these issues.

2. Revoking Authorization

a. The Client has the right to revoke his or her authorization at any time for any reason. If the Client wishes to revoke the client authorization, the Client must make its request in writing. Additionally, the Agency will need to contact IHCDA so that it can determine the best process to use to deny access to the Client's file in HMIS.

G. DATA PROTOCOLS:

1. The Agency must collect the Universal Data Elements as defined by HUD. Agencies receiving certain types of funding may also be required to collect the Program Data Elements as required by HUD or IHCDA. Finally, IHCDA may identify other data elements that the Agency will be required to submit.

2. Data must be entered into the HMIS within fourteen (14) days of data collection as provided for in the **HMIS Participation Agreement**.

3. Agency Users shall ensure all information entered and stored in the HMIS is accurate. Entry of intentionally inaccurate information in the HMIS may result in revocation of an Agency User's license or licenses.

4. If an Agency User does not have the information for a particular data field, he or she must not enter any incorrect values, but shall wait to complete the screen until answers to all data fields are known. If at all possible, data entry must be performed while the Client is present.

5. The Data Collection and Evaluation Committee is actively involved in making suggestions, improvements and modifying the processes for HMIS and data quality. The Data Collection and Evaluation Committee annually makes a recommendation to the CoC Board about a specific data quality plan.

H. AGENCY PARTNER AGREEMENT:

The Executive Director or authorized official must sign the **HMIS Participation Agreement**, which confirms the Agency's commitment to comply with the policies and procedures for using the HMIS and

collaboration with IHCDA. The current **HMIS Participation Agreement** is posted at www.in.gov/myihcda/2444.htm.

I. ENFORCEMENT OF PROPER USE OF THE HMIS:

All Agency Users must sign the **HMIS User Agreement/Code of Ethics and** comply with the terms contained in it whenever using the HMIS. Violation of this agreement may be considered a violation of the Agency User's employment with the Agency, and could result in disciplinary action, up to and including termination of the Agency User's employment or affiliation with the HMIS as well as potential personal civil and criminal legal fines and penalties. The current **HMIS User Agreement/Code of Ethics** is posted at www.in.gov/myihcda/2444.htm.

J. IMPLEMENTATION ASSESSMENTS

Agencies may be monitored/ audited on compliance with the procedures outlined in HUD's HMIS Data and Technical Standards and the policies and procedures contained herein.. Agencies should conduct a self-assessment by downloading the current **HMIS Security Audit Checklist** at http://www.in.gov/myihcda/2444.htm.

Access Privileges to HMIS

Policy:	HMIS Staff and participating Agencies will apply the Agency User access privilege practices set forth in this procedure as well as enforcing access privileges to the HMIS servers.

Procedure:

HMIS User Agreement/Code of Ethics must be signed by each Agency User, whether the User is a staff member, volunteer or consultant prior to the Agency User receiving HMIS training and a password to the HMIS. A copy of the **HMIS User Agreement/Code of Ethics** must be sent to IHCDA and IHCDA will maintain a copy of it.

User Access Privileges to HMIS

A. AGENCY USER ACCESS:

Agency User access and access levels may be determined by the executive leadership of the Agency in consultation with the Agency Executive User. HMIS Staff will generate usernames and passwords for each Agency User, who will be required to generate a unique password his or her first time accessing the HMIS. The Agency User should be the only person, who will know his or her unique password.

Agency Users are bound by the **HMIS User Agreement/Code of Ethics** and the **HMIS Participation Agreement** and must comply with same. All Agency Users have a critical role in the effort to protect and maintain Client information contained in the HMIS.

Agency Users have the following responsibilities:

1. Agency workstations should be configured to automatically turn on a password protected screen saver when the workstation is temporarily not in use.
2. Agency Users must log off the HMIS or lock their workstation when leaving their work station and close the Internet browser to prevent someone else from viewing the last Client screen.
3. Read and sign the **HMIS User Agreement/Code of Ethics** when joining an Agency and as directed by IHCDA based on policy updates.
4. Support compliance with all federal and state statutes and regulations.
5. Maintain the confidentiality, privacy and security of PPI that have collected or for which Agency Users have been given access privileges
6. Accept responsibility for all activities associated with the use of their Agency User accounts and related access privileges.
7. Report all suspected security and/or policy violations to an appropriate authority at the Agency (e.g., manager, supervisor, system administrator or the HMIS Security Officer). Utilize the security incident report form and send in writing to the HMIS manager at IHCDA.
8. Review the **HMIS Notice of Privacy Practices**, the **HMIS Statement of Privacy Practices** and the **HMIS Policies and Standard Operating Procedures**.
9. Attend all trainings required by IHCDA HMIS policies and guidance.
10. Follow all specific policies, guidelines and procedures established by the Agency with which they are associated and that have provided them access privileges.

Persons who violate this policy may be denied access to HMIS and may be subject to other penalties and disciplinary action. The Agency should have documented procedures in place for issuing, altering, and revoking access privileges on shared systems. Any Agency User's right to access the HMIS shall be at IHCDA's sole discretion.

B. IHCDA USER ACCESS:

Only IHCDA staff needing information from the HMIS for legitimate business purposes shall be given access rights. Prior to being given access rights, he or she shall be trained on HMIS privacy and security policies and sign the **HMIS User Agreement/Code of Ethics**.

C. PASSWORDS:

1. An Agency shall only permit access to HMIS with use of an Agency User authentication system consisting of a username and a password which the Agency User may not share with others. Temporary passwords are created when a new Agency User is created.
2. The Agency User will be required to change the password the first time he or she logs into the system. Passwords are the individual's responsibility and Agency Users cannot share passwords and passwords should be stored securely and not be accessible to other persons. Passwords should never be stored or displayed in any publicly accessible location. Passwords should be designed to prevent any Agency User from being able to

log onto more than one (1) workstation at a time, and to prevent any Agency User from being able to log onto the network from more than one (1) location at a time.

3. The password must be between 8 and 12 characters and contain a mix of alpha and numerical characters (alphanumeric). Passwords should not use or include the User's username, the HMIS name, or the HMIS Software Vendor's Name. Passwords should not be easily guessed or consisting entirely of any common word found in any dictionary (spelled in correct or reverse order).

4. Passwords should be changed periodically by each Agency User. IHCDA requires that HMIS passwords are changed at least every ninety (90) days.

    a. The Agency Executive User must immediately notify IHCDA staff of the any Agency User's termination to allow IHCDA staff to terminate the Agency User's access rights. If a staff person is planning to go on leave for a period of longer than forty-five (45) days, their password should be inactivated immediately upon the start of their leave. User accounts will automatically terminate after thirty (30) days of inactivity.

D. ELECTRONIC TRANSMISSION OF USER IDENTIFICATION AND PASSWORDS:

No one shall engage in electronic transmission of Agency User ID's and passwords, including temporary passwords, without the approval of IHCDA. Authenticators will be transmitted only by surface mail, phone, or in person unless otherwise approved by IHCDA.

E. TRACKING OF UNAUTHORIZED ACCESS:

IHCDA or its subcontractor will periodically review all HMIS and the HMIS Software Vender security logs, including, where available, the transactions log, the Internet log, the log of web server errors, the firewall log, tracking attempts at unauthorized access at the direction of the HMIS Security Officer. The IHCDA's HMIS Software Vendor shall establish attempt thresholds to ensure HMIS security. IHCDA will follow up with Agencies when the logs reveal questionable activity at its location and may require corrective action to be taken by any such Agency.

Unauthorized access is prohibited and may prompt IHCDA to take legal action.

Security

Policy:	Access to all computing, data communications and sensitive data resources will be controlled. Access is controlled through user identification and authentication. Agency Users are responsible and accountable for work performed and actions taken in HMIS with their username. Access control violations must be monitored, reported and resolved. Agency staff must work to ensure that all sites receive the security benefits of the system while complying with all HMIS policies

A. PROCEDURES:

1. To protect the availability, security, and integrity of the HMIS, all computing systems (including, without limitation, networks, desktops, laptops, mini-computers, mainframes, and servers) accessing the HMIS or containing personal protected information shall comply with the minimum security measures and practices outlined herein.

   The procedure for client data generated from the HMIS shall be that electronic data shall be stored in a binary, not text, format. Protected Personal Information shall be stored in an encrypted format using at least a 128-bit key. Regarding raw data: Agency Users who have been granted access to the HMIS report functionality have the ability to download and save Client level data onto their local computer. Once this information has been downloaded from the HMIS in raw format to an Agency's computer, this data becomes the responsibility of the Agency. An Agency must develop a protocol regarding the handling of data downloaded from the report writer, record disclosure and storage.

2. The HMIS is a secure database which allows twenty-four (24) hour access to all qualified Users. The Agency must develop and enforce policies and procedures to address the following areas of data security and integrity:

B. PHYSICAL SECURITY:

In order to ensure that unauthorized persons cannot physically access servers, physical security measures and objectives will be implemented where applicable and appropriate to protect HMIS computing and network assets. As with logical security measures at IHCDA, physical security measures required for protecting the HMIS computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved. The more sensitive and critical the computing environment, the more control measures are likely to be used. Because HMIS will be collecting and storing sensitive information, physical access control measures sufficient to prevent the HMIS from unnecessary and unauthorized access, use, misuse, vandalism, or theft must be implemented. All specific tools, systems, or procedures implemented to meet physical security requirements should be selected on the basis of its cost-effectiveness and common sense.

IHCDA's HMIS Software Vendor and data custodian shall provide the following security, as well as follows all other security measures set forth herein:

1. HMIS data shall be copied on a regular basis to another medium (*e.g.*, tape) and stored in a secure off-site location. Ideally, the regular copying will be via continual redundant backups.

2. Off-site storage shall include fire and water protection for the storage medium.
3. Surge suppressors shall protect physical systems for collecting and storing the HMIS data.
4. Central server, mainframe or mini-computer shall store the central hardware in a secure & locked room with an uninterrupted power supply, a raised floor, and appropriate temperature control and fire suppression systems.
5. Electronic data transmission transmitted over publicly accessible networks or phone lines shall be SSL encrypted to at least 128-bit encryption.
6. Electronic data shall be stored in a binary, not text, format. Protected Personal Information shall be stored in an encrypted format using at least a 128-bit key.
7. Access to the physical system shall be controlled.
8. Network redundancy built into central server site and/or alternate site.
9. Staff on site or on call 24x7.
10. Server firewall and virus protection shall be maintained and kept current.

C. USER SECURITY

Agency must address the following areas:

1. Agency Policies Restricting Access to Data: Each Agency must establish internal access to data protocols. These policies must govern who has access, for what purpose, and how the information can be transmitted. Other issues that should be addressed include storage, transmission and disposition of this information. Agencies must have written policies and procedures in place regarding the appropriate access to Client data in the HMIS and its obligations herein and the under **HMIS User Agreement/Code of Ethics**. The policies must include, without limitation, when, where and under what circumstances it is deemed appropriate for Agency staff to access HMIS data outside the office. The policies must also indicate the consequences for an individual's failure to abide by these policies.
2. Raw Data: Agency Users who have been granted access to the HMIS report functionality have the ability to download and save Client level data onto their local computer. Once this information has been downloaded from the HMIS in raw format to an Agency's computer, these data then become the responsibility of the Agency. An Agency must develop protocols regarding the handling of data downloaded from the report writer, and disclosure and storage of these records.
3. The HMIS software will automatically log off after a pre-set interval of inactivity.
4. The use of this HMIS constitutes an express consent to the monitoring of system use and security at all times. If such monitoring reveals possible violations of the law, pertinent information will be provided to law enforcement officials. Any persons using HMIS or information obtained from this application, without proper authorization or in violation of these policies and procedures may be subject to civil and/or criminal prosecution. Any persons enabling access by an unauthorized individual may also be subject to internal disciplinary actions in addition to civil and/or criminal prosecution.

5. These policies are applicable to all users (employees, contractors, and others) of agencies, partners and funders and the computer systems, networks, and any other electronic processing or communications and related resources used in conjunction with the IHCDA HMIS system and/or data obtained through the HMIS system.

6. Each person with access to confidential information must understand their personal responsibility to maintain its confidentiality. Client information must be protected so that it cannot be modified while in transit or storage. Reported data must be accurate. If an employee leaves your agency, inform IHCDA within two (2) business days that their account can be deactivated.

7. Users may not electronically transmit unencrypted client data across a public network. Users must use the following procedures:

    a. Data extracted from HMIS and stored locally will be stored in a secure location and will not be transmitted outside of the private local area network unless it is properly protected.
    b. Personal identifiable client data will not be distributed through email.
    c. User must clear browser history once he or she logs out of HMIS
    d. Do not allow the browser to save password.

    e. Any security questions can be addressed to the HMIS System Administrator.

D. MEDIA AND HARDCOPY PROTECTION:

The Agency must secure any electronic media or hard copy containing identifying information that is generated either by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. Any paper or other hard copy generated by or for the HMIS that contains identifying information must be supervised at all times when it is in a public area. If Agency staff is not present, the information must be secured in areas that are not publicly accessible in a secure manner (*e.g.*, locked filing cabinet or locked office). Agencies wishing to dispose of hard copies containing identifying information must do so by shredding the documents or by other equivalent means with approval by IHCDA. In addition, in order to delete data from a data storage medium, the Agency must have procedures that require the reformatting of the storage medium. The data storage medium should be reformatted more than once before reusing or disposing of the medium.

E. AGENCY USER AUTHENTICATION:

Authorization is the provision of specific permissions or authority to have access. Access control measures required for establishing Agency Users' access to any HMIS computing resources shall be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved. All Agency Users' system access must be based on the "principle of least privilege" and the "principle of separation of duties."

There will be multiple levels of access to the HMIS. The appropriate access to the HMIS is determined for each Agency User. This determination is to be based on each Agency User's job function as it will

relate to the HMIS data entry and retrieval and will be officially designated by the Agency Executive User.

The HMIS will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent the interception of critical or sensitive information.

F. CONFIDENTIALITY

The HMIS preserves confidentiality by encrypting the data sent over the Internet. In addition, the Agency must make every effort through its policies and procedures to ensure that any PPI collected remains confidential, especially at the intake point.

Any staff, volunteer or other person who has been granted an Agency User ID and password and has committed a breach of security of HMIS and/or Client confidentiality may be subject to sanctions including but not limited to a warning or revocation of HMIS access rights. A revoked Agency User may be subject to discipline by the Agency pursuant to the Agency's personnel policies.

Federal, state and local laws seek to protect the privacy of persons with physical and/or mental illness, who have been treated for alcohol and/or substance abuse, have been diagnosed with HIV/AIDS, Agencies who serve these protected classes of clients, may hide the Client's case notes, diagnoses, and treatment hidden from other agencies using the HMIS. The Agency is encouraged to seek its own legal advice in the event of requests of this PPI by other agencies.

G. INTEGRITY

Integrity provides assurance of an unaltered or unmodified state of information. All systems are required to have the capability to log basic information about an Agency User and access activity and for the possible creation of historical logs and access violation reports. The Agency Executive User should review audit reports periodically to ensure appropriate privacy and data access policies are being followed. Deviations from policy should be reported to IHCDA at within twenty-four (24) hours of discovering the inappropriate access.

H. AVAILABILITY

Availability ensures that there is no delay or denial of authorized services or loss of data processing capabilities. This takes into account things such as virus protection, firewalls, intrusion detection, management of operating system updates, backup and recovery, and physical security to make sure that HMIS is available to be used by Agency Users.

I. COMPUTER OPERATING SYSTEM MAINTENANCE

Agencies must have a plan to keep the computers used to access HMIS updated with the latest security and other updates recommended for the operating system. The local and server network computers must have automatic updates on every computer that accesses HMIS.

J. FIREWALLS AND VIRUS PROTECTION

Agencies must have firewall protection on its networks or computers providing a barrier between the organization and any systems, including the Internet and other computer networks, located outside of the

organization accessing the Internet and the application. For example, a workstation that accesses the Internet directly through a modem would need a firewall; however, a workstation that accesses through a central server would not need a firewall as long as the server has a firewall.

Virus protection must also be in place employing commercially available virus protection software that includes automated scanning of files as they are accessed by Agency Users on the system where the HMIS application is housed. Each Agency and IHCDA must also subscribe to virus software, as well as an updates subscription to maintain the virus definitions and code base.

K. PERSONNEL SECURITY MEASURES

Agencies must establish and maintain all necessary processes and procedures to properly and immediately close and remove all system and network privileges and resources when an employee is terminated including notifying IHCDA to disable the account.

L. DISASTER PROTECTION AND RECOVERY

The HMIS is redundantly and physically backed up by the HMIS Software Vendor in accordance with all current HUD requirements. It is recommended that larger Agencies consider their own back up of any HMIS data maintained on site. All Agencies should have a disaster plan that allows uninterrupted business access to the Internet for the purposes of the HMIS despite fire, flood or other disaster.

M. SECURITY VIOLATIONS

1. All security breaches must be reported first to the HMIS Manager. As appropriate IHCDA legal department will be made aware of the situation. The Attorney General will be notified if any social security breaches are made as required by Indiana law.
2. Upon notification of a security breach, the IHCDA HMIS Manager will investigate the report. IHCDA's systems analyst, currently At Work Solutions, will investigate the technical issues in collaboration with IHCDA's IT department. The systems analyst will document the situation and how the problem has been corrected. Testing will be conducted to ensure that the problem has been resolved. If the security breach involves PPI IHCDA's legal department will be notified and will provide guidance on any specific actions that need to be taken by the Agency.
3. IHCDA will report and respond to security incidents by following HUD-determined predefined threshold when reporting is mandatory, as established by HUD.
4. If during the cost of auditing it is determined that an Agency has a HMIS policy or security violation, the Agency must respond to IHCDA in writing within 10 working days after notified of the HMIS Policy Violation (breach in security) or the incident is discovered by the Agency. The Agency must inform IHCDA of how it has addressed the violation. Failure to comply with HMIS requirements may result in IHCDA withholding program payments until compliance is completed and documented, or termination of the grant(s). In addition, failure to comply with requirements may result in an Agency being ineligible for funding or receiving a low HMIS performance score in the next grant year.

N. NON HUD FUNDED AGENCIES:

00009951-1

Agencies that are not funded by HUD programs but utilize HMIS must comply with the same policies and procedures as Agencies that are funded by HUD. Failure to comply may result in termination of the Agency's access to HMIS.

O. DESK AND/OR ONSITE MONITORING

IHCDA staff will monitor HMIS participation through periodic and annual desk and/or onsite security reviews to ensure the implementation of the security requirements. Additionally, data in HMIS will be reviewed regularly. Data will be reviewed within the reimbursement process for HUD sponsored permanent supportive housing programs. IHCDA reserves the right to withhold payment until HMIS violations are corrected or required levels of data quality are achieved. IHCDA will also review data quarterly for all other BoS CoC HUD Grantees. Data quality and project performance will be reviewed by the CoC for all projects.

IHCDA will provide a security audit checklist for the security reviews to provide Agencies with expectations for monitoring. The goal of the audits is to ensure that Agencies are complying with security requirements. IHCDA will work with agencies with that receive findings to ensure they are remedied as quickly as possible for the benefit of all Agencies who utilize HMIS.

Consequences of Security Violations:

- Findings will be assessed for the security breach. These issues must be resolved by the date specified by IHCDA. The Agency may be warned and/or additional training may be required.
- Second time offense – The Agency's access to HMIS may be suspended, points may taken away from current or future funding applications, or an Agency may be required to assign the right to use/ enter their Clients information to another individual or entity

Agency Implementation Assessments and Denial of User or Participating Agency Access

Policy:	An Agency or an Agency User's access may be suspended or revoked for a suspected or actual violation of HMIS privacy or security protocols. IHCDA shall perform random Implementation Assessments of Agencies. Serious or repeated violations by Agency Users of HMIS privacy and/or security guidelines may result in the suspension or revocation of an Agency's access.

Procedure:

A. AGENCY RESPONSIBILITY

1. Agencies are responsible for understanding and ensuring that their Agency Users abide by the following policies posted on www.in.gov/myihcda/2444.htm.
    a. **HMIS User Agreement/Code of Ethics;**
    b. **HMIS Privacy Practices Notice**

c. **HMIS Statement of Privacy Practices;**

d. **HMIS Standard Operating Procedures;**

e. **HMIS User Agreement/Code of Ethics;**

f. **HMIS Participation Agreement**; and

g. Any other policies or guidance issued by IHCDA.

2. Agencies must pass the Security Audits performed by HMIS Staff or perform remedial actions that are required to pass the Security Audits within the time period provided requested by IHCDA.

3. Agencies may self-assess by downloading the current Security Audits Checklist on http://www.in.gov/myihcda/2444.htm.

B. IHCDA STAFF PROCEDURE:

1. IHCDA shall perform random Security Audits following the **Security Audit Checklist**. These audits may occur in conjunction with other monitoring or inspections performed by IHCDA that is not specific to the HMIS.

2. IHCDA shall call the Executive Director or Executive Agency User to arrange a time to meet. If the Executive Director or the Executive Agency User is not available, another Agency staff member familiar with the HMIS operation should accompany IHCDA during the Implementation Assessment.

3. Violations of security or privacy protocols will be investigated by the Agency and HMIS Staff.

4. All confirmed violations of a breach of a Client's PPI will be communicated in writing by the Agency to the affected Client within fourteen (14) days, unless the Client cannot be located. If the Client cannot be located, a written description of the violation and efforts to locate the Client will be prepared by the Agency, and sent to IHCDA and placed in the Client file at the Agency.

5. If the Agency fails the audit and follow up work is required, the proposed next audit date will be negotiated, and the corrective actions will need to be completed prior to the next Implementation Assessment.

6. Any Agency User found to be in violation of security protocols may be sanctioned accordingly. Sanctions may include but are not limited to: submission of a plan of correction, a formal letter of reprimand, suspension of HMIS privileges, revocation of HMIS privileges, termination of the HMIS Participation Agreement, and civil or criminal prosecution.

7. All sanctions will be imposed by IHCDA.

8. All sanctions may be appealed to the Data Collection and Evaluation Committee to receive a non-binding advisory opinion on whether the sanction is appropriate. In all cases, IHCDA retains the final discretion and authority to impose sanctions.

9. Additional sanctions may be imposed by funders.

Notwithstanding these Implementation Assessments and other auditing being performed by IHCDA and the procedures described herein, IHCDA may take action for violation of the procedures described herein even if the violation is discovered by IHCDA through other means.

HMIS Training

Policy:	HMIS Staff will conduct and oversee training to new and existing Agency Users.

Procedure:

HMIS Staff are the primary responsible party for training Agency Users. The training administered by HMIS Staff is required by all HMIS users at least annually, as verified by registration for and attendance at a scheduled webinar training hosted by IHCDA. Training webinars are offered on a variety of topics and to audiences that include new users and advanced users interested in executive level reports and/or preparation of required Annual Progress reports or other reports required by HUD. HMIS trainers include IHCDA staff, representatives of ClientTrack and other contracted consultants.

New Users: Prior to issuance of a user password each new user must complete the User Agreement/Code of Ethics and return it to IHCDA, preferably via email. Upon receipt and after training, HMIS Staff will issue a user name and initial password. All users are expected to be active on the HMIS and to have attended training at the very least annually.

Established Users: All HMIS users are required to attend at least one (1) training session annually. The training topic must include security training but does not need to be a repeat session of new user training.

Training: Participation in training will be evidenced by the logs maintained for on line webinars and/or sign in sheets at live trainings. Any Agency User found to be logging in to training but not actively following the session, as evidenced by electronic monitoring of alternate key stroke activity, failure to connect and other open windows, will be required to repeat the training.

HMIS User License Billing

Policy:	Agencies serving the Homeless shall have access to the IHCDA maintained HMIS for free. There is no requirement that an agency receive HUD or other federal or state funds to participate in the HMIS. IHCDA reserves the right to charge a reasonable fee for the use of the HMIS for other purposes.

Procedure:

A. BILLING:

1. Any billing of User licenses by IHCDA that occurs related to use of the HMIS will be in accordance with this section.

B. TERMINATING OF USER LICENSES:

1. Refunds or partial refunds will not be given to any Agency when a User license is terminated due to a violation of HMIS policies and procedures.
2. Refunds or partial refunds will not be given to any Agency when a User license is terminated in the middle of the twelve (12)-month billing cycle for that license except at IHCDA's sole discretion and in the case of rare and extenuating circumstances.

C. TRANSFERRING USER LICENSES:

1. Agencies may terminate one (1) User license and add another license simultaneously without disrupting the billing cycle or incurring any additional costs. For example, if an Agency User needs to take a leave of absence, another Agency User can be added during that time period.
2. All licenses that are transferred must have a new username and password created.
3. All Agency Users must sign the **User Agreement/Code of Ethics** and return a copy the agreement to IHCDA prior to receiving a username and password.
4. All new Agency Users must attend HMIS training. Training may be provided onsite by an individual authorized by IHCDA. Agency User may also attend one of IHCDA's training sessions.

D. CANCELLATION OF USER LICENSE:

1. Agencies may cancel a User license within thirty (30) days of its creation, or within thirty (30) days of receiving an invoice for a User license, at no charge.
2. Agencies that cancel User licenses may be assessed fees that have been previously waived, such as training fees and setup fees.

HMIS Technology Requests

Policy:	Agencies may request assistance from IHCDA to purchase computers, manage special programs, improve Internet connections, and address other technology issues. IHCDA will establish a policy to solicit and evaluate these technology requests. Assistance may be provided based on availability of funding and at IHCDA's sole discretion.

Procedure

A. AGENCY PROCEDURE:

1. Agency must complete and submit a technology request via e-mail.
2. IHCDA will review and consider the request. Technical requests not requiring additional funds will be evaluated by HMIS Staff and responded to directly. When the request

involves the purchase of equipment and/or costs related to outside consultation, it will be reviewed by IHCDA on a case by case basis.

3. If the request for funding is approved, the Agency may incur the cost and/or submit documentation to IHCDA for reimbursement.
4. IHCDA will review all requests and develop a timeline for approval and implementation.
5. Incomplete or denied requests may be resubmitted.

Data Collection and Evaluation Committee

Policy:	A Data Collection and Evaluation Committee was formed to review and/or create policy and resolve issues associated with the HMIS.

Responsibilities:

The Data Collection and Evaluation Committee is a committee of the Planning Council on Homelessness and the CoC Board and, as such, advises and supports the HMIS operations in resource development, consumer involvement, quality assurance and stakeholder accountability. The IHCDA designated the Data Collection and Evaluation Committee and the CoC Board to assume the aforementioned roles. While the Data Collection and Evaluation Committee has been given responsibility for oversight of the HMIS, IHCDA is the final decision making authority on policy for the HMIS.

Membership Guidelines:

Membership on the Data Collection and Evaluation Committee shall be by invitation only from IHCDA. The Data Collection and Evaluation Committee was established according to the following guidelines:

1. Target membership will be ten (10) persons.
2. The membership shall represent the geographical mix of state-wide Agencies.
3. There will be a proactive effort to have representation from consumer representatives, shelter/transitional housing for families and individuals, other homeless services organizations and government agencies that fund homeless assistance services.
4. There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the HMIS.
5. The term of a member of the Data Collection and Evaluation Committee will be evaluated by the the CoC Board.

Meeting Frequency:

The committee shall meet monthly or more frequently, as needed.

Procedure

IHCDA staff shall:

00009951-1

1. Schedule the meeting, provide a physical location and a dial in phone number.
2. Provide administrative support for the meetings, including the agenda, printing meeting materials and recording minutes of the meeting in a timely manner.

The Committee shall:

1. Receive and review reports from the HMIS.
2. Authorize and review the results of HMIS user surveys.
3. Review changes necessitated by amendments in HUD Data Standards.
4. Periodically conduct an assessment of the present software and its HMIS Software Vendor and make recommendations as to its continuing or change.
5. Review and approve the annual HUD NOFA application for funding, as well as the Annual Progress Report.
6. Provide expert assistance to other Planning Council Committees in support of their data driven decisions.
7. Actively explore and promote data exchange between State and other type of agencies with the goal of improving services to homeless persons.

Data Use and Disclosure

Policy:	The purpose of this policy is to specify how information collected by HMIS will be used or disclosed and under what conditions the information may be accessed. It categorizes the data that HMIS Staff will administer and indicates the controls required to ensure data integrity as information is shared.

Responsibilities:

Each HMIS Stakeholder has certain rights and responsibilities regarding the data collected within the HMIS.

A. HMIS SPONSORS

HMIS sponsors have rights to all De-Identified Public Data produced through the HMIS. Sponsors are:

- United States Department of Housing and Urban Development
- Indiana Housing and Community Development Authority

B. HMIS STAFF

HMIS Staff is responsible for the proper collection and dissemination of information among the HMIS Stakeholders. The HMIS Staff is responsible for ensuring that all Client information is fully protected and that all data use conforms to IHCDA adopted policies.

C. AGENCY USERS

00009951-1

Agency Users are also responsible for ensuring that all Client information is fully protected and that all data use conforms to IHCDA adopted policies.

D. AGENCIES AND PROGRAMS

Agencies sign the **HMIS Participation Agreement** (posted on http://www.in.gov/myihcda/2444.htm) pledging their agreement and support of all policies. Agencies also agree to post the **HMIS Statement of Privacy Practices** that defines the rights of Clients and contact information should a Client want to revoke access to his or her PPI.

Procedure:

A. ALLOWABLE USES AND DISCLOSURES OF PROTECTED PERSONAL INFORMATION ("PPI")

1. Privacy Documents:
   a. The **HMIS Notice of Privacy Practices** describes for Clients why personal information is being collected and refers Clients to the **HMIS Statement of Privacy Practices** for additional information regarding how this information may be used or disclosed.
   b. The **HMIS Statement of Privacy Practices** describes how information about Clients can be used and disclosed and how Clients can access their information.
2. Routine Uses and Disclosures: PPI in the HMIS may be used and disclosed under the following routine circumstances:
   a. Coordination of Services: PPI may be used and disclosed to provide or coordinate services to a Client.
   b. Payment: PPI may be used and disclosed for functions related to payment or reimbursement for services.
   c. Administrative Functions: PPI may be used and disclosed to carry out administrative functions, including, but not limited to legal, audit, personnel, oversight, and management functions.
   d. Creating De-Identified PPI: PPI may be used and disclosed to create De-identified Information.
3. Other Permissive Disclosures: The following additional uses and disclosures recognize those obligations to disclose PPI by balancing competing interests in a responsible and limited way. These additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this paragraph modifies an obligation under applicable law to use or disclose PPI. The following uses and disclosures of PPI may only be made upon the approval of the Executive Director of the Agency and in consultation with IHCDA:
   a. Uses And Disclosures Required By Law: PPI may be used and disclosed when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

b. Uses And Disclosures To Avert A Serious Threat To Health Or Safety: PPI may be used and disclosed, consistent with applicable law and standards of ethical conduct, if: (1) IHCDA, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

c. Uses And Disclosures About Victims Of Abuse, Neglect Or Domestic Violence: PPI about an individual whom agency staff reasonably believes to be a victim of abuse, neglect or domestic violence may be disclosed to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:

(1) Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;

(2) If the individual agrees to the disclosure; or

(3) To the extent that the disclosure is expressly authorized by statute or regulation; and the agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

If such a permitted disclosure about victims of abuse, neglect or domestic violence is made, staff must promptly inform the individual that a disclosure has been or will be made, except if: (1) the Executive Director of the Agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or (2) staff would be informing a personal representative (such as a family member or friend), and the Executive Director of the Agency reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the Executive Director of the Agency, in the exercise of professional judgment.

d. Uses And Disclosures For Academic Research Purposes: PPI may be used and disclosed for academic research conducted by an individual or institution that has a formal relationship with IHCDA if the research is conducted either:

(1) By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by the Program Director (other than the individual conducting the research); or

(2) By an institution for use in a research project conducted under a written research agreement approved in writing by the Program Director.

All uses and disclosures for Research purposes shall comply with subsection E below ("IHCDA HMIS Research Policy"). Further, a written research agreement must: (1) establish rules and limitations for the processing and security of PPI in the course of the research; (2) provide for the return or proper disposal of all PPI at the conclusion of the research; (3) restrict additional use or disclosure of PPI, except where required by law; and (4) require that the recipient of data formally agree to comply with all terms and conditions of the agreement. A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

e. Disclosures For Law Enforcement Purposes: PPI may be disclosed, consistent with applicable law and standards of ethical conduct, for a law enforcement purpose to a law enforcement official under any of the following circumstances:

(1) In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

(2) If the law enforcement official makes a written request for protected personal information that: (1) is signed by a supervisory official of the law enforcement agency seeking the PPI; (2) states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PPI sought; (4) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (5) states that de-identified information could not be used to accomplish the purpose of the disclosure.

(3) If IHCDA believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of IHCDA or an HMIS Agency;

(4) In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or

(5) If (1) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and (2) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

B. DATA ACCESS

1. HMIS Staff: HMIS Staff may have access to all data types (including, but not limited to PPI) as necessary to perform their functions for the HMIS and consistent with the Routine Uses and Disclosures listed in "A" above. HMIS Staff must pass a background check and sign the **HMIS User Agreement/Code of Ethics**.

2. HMIS Sponsors' Representatives: HMIS sponsors' representatives may receive reports containing Public Data.

3. HMIS Subcontractors and Vendors: HMIS subcontractors and vendors have access to all data types as necessary to perform their functions for HMIS consistent with the Routine Uses and Disclosures listed in "A" above. HMIS subcontractors and vendors must agree in writing to maintain the confidentiality of all data received from HMIS.

4. HMIS Agencies and Programs: Agency and program staff have access to their own Agency's/program's data, as bound by these HMIS Policies and Standard Operating Procedures. Agency and program staff must sign the **HMIS User Agreement/Code of Ethics** and agree to follow these Policies and Standard Operating Procedures. HMIS Agencies and programs may also have access to Public Data and PPI submitted by other Agencies for purposes of providing services to a Client (with implied Client consent), except under circumstances where federal or state law requires additional restrictions or confidentiality protections.

5. Access to Data for monitoring: A regional CoC representative may have access to Agency data for the express purpose of monitoring and aggregate reporting purposes for regional review. A current and signed MOU must be in place in order for a regional CoC representative to have access to data for an Agency.

6. Researchers: Researchers may have access to PPI and De-identified Information only in accordance with the approval procedures set forth below in "E" ("IHCDA HMIS Research Policy").

7. Other Third Parties: Data may be disclosed to other third parties (*e.g.*, media requests) only in accordance with the approval procedures set forth below in "D" ("Public Data Releases").

C. IHCDA DATA PROCESSING & PREPARATION

IHCDA may or may not do the following:

1. Cleaning: Data cleaning may be performed by HMIS Staff, a subcontractor, or another IHCDA vendor. During this process the data is reviewed for completeness, adherence to the data schema (data types and answer ranges), and consistency with prior data releases.

2. Preparing Data: Usually some data modification is needed before it is shared. For any data that will be shared outside the Agency of origin, data preparation will include the removal of all identifying and confidential information. In addition, case filtering, data element selection or other preparation may be needed prior to data release. This is often the case when preparing data for reports or for use by analysts that are focusing on specific populations or topics. Data subsets may be extracted according to time period, Agency, Agency type or any other dimension contained within the database.

3. Data Tagging: Each data release must be accompanied by information describing the data source, time period covered, geographic area covered, and populations included. Also, any known data limitations and any context vital to accurately interpreting the data should be included.

D. PUBLIC DATA RELEASES

1. Public Data Release Procedure:

   a. HMIS Manager Role: The HMIS Manager shall approve or deny the general format and content of reports that contain Public Data that will be released. When a report meets the requirements of such a pre-approved format, no further HMIS Manager approval is required. However, if a report does not meet such a pre-approved format, HMIS Manager's approval shall be required and the HMIS Manager shall respond to such requests for Public Data, coordinating efforts and serving as a resource to other staff and providing information to Clients regarding use and disclosure of their Protected Personal Information collected, received, used, or disclosed by the HMIS. If IHCDA administration denies an external party access to the HMIS data or adds unacceptable modifications, that party may petition the IHCDA Data Collection and Evaluation Committee to review and possibly overturn the decision. The Committee's decision shall be in its sole discretion and shall be final. The external party shall have no further right to appeal. The HMIS Manager shall ensure that HMIS Staff maintains a log of the dates and content of any reports of Public Data that are generated and released.

   b. Certify Readiness: The HMIS Manager must approve every data or report release and must determine that the data is statistically valid for sharing. There is no one standard test; it is a judgment call made by professionally trained database specialists under management of or contracted by IHCDA. However, one statistical test might be sufficient coverage of the data subsets involved (*e.g.*, at least 60% of all data parameters). The data must meet Minimum Necessary level either pre-determined by formal thresholds, or established based on the HMIS Manager's judgment or by the judgment of a professional data analyst hired for the purpose of certifying HMIS data. If Public Data is to be released that is not statistically valid, appropriate caveats and context must be attached to the data.

2. Types of Public Information Released: There are several types of Public Data that may be released. Information that may be released is Aggregated Data and some Client-level De-identified Information.

   a. Aggregated Data

      (1) **Pre-set Summary Reports** – simple reports of predefined information and timing released to agencies, funders' analysts, and other Stakeholders.

      (2) **Required Reports** – including the Annual Performance Report (APR) for the U.S. Department of Housing and Urban Development and other agreed upon reports required by local funders, county, state and federal organizations.

      (3) **Ad-Hoc Reports** – including HMIS-generated reports such as "Community Snapshots," progress reports, average length of stay reports.

      (4) **Participation Reports** The following shall apply to Participation Reports:

- IHCDA will use the Housing Inventory Chart of the Continuum of Care ("CoC") in Indiana to determine the number of Emergency Shelters, Transitional Housing, and Permanent Supportive Housing programs in each CoC Region.

- IHCDA will publish lists of programs that are participating in the HMIS and distribute the list to local and regional CoC networks, city leaders, and other key organizations.

b. Client-level Data

- **Data Tables** – De-identified Client-level data to be used for subsequent data analysis. Often the tables are only a selected sample (usually filtered for Client population, time period, service type or something similar) of the total cases available. Data tables are only available under the following conditions:

  i. the users are certified and pre-approved and,

  ii. a written request to disclose data is submitted and approved by HMIS Manager; such requests may be on-going.

3. Release Notification: The following actions will be taken whenever HMIS generated data or report is released to the general public or to parties not directly participating in the HMIS, except for Ad-Hoc and Participation Reports as described above.

   a. In the case of released reports, identified agencies and programs will be given the opportunity to review and comment on the reports before public release.

   b. In the case of released reports, notification will be posted on the IHCDA web site at the time of release.

   c. The Data Collection and Evaluation Committee will regularly be given reports summarizing the data access requests and permissions, and the report releases.

4. IHCDA HMIS Data Release Charge: Because there are costs in generating data files or reports, IHCDA may charge external parties for the costs occurred in generating the requested data. These costs may include but are not limited to: analyst time, printing costs, and computer time, among others.

E. IHCDA HMIS RESEARCH POLICY

As a general policy, IHCDA shall not disclose Protected Personal Information for Research purposes. Upon receipt of a request for Protected Personal Information for Research purposes, HMIS Staff may provide the requesting person or entity with De-Identified Information that will allow the requestor to identify cohorts of Research subjects at individual Agencies. The requestor may then contact individual Agencies to request Protected Personal Information for purposes of the Research Activity. Notwithstanding the foregoing, the Personal Protected Information may be disclosed by HMIS Staff for Research activities pursuant to the following procedures:

1. Access to Data: External parties must apply and have written permission from IHCDA administration prior to the start of Research activity involving Protected Personal Information or De-identified Client Information. IHCDA's HMIS Manager and Data Analyst will generally make the determination on data access.

   a. Approval will be conditioned upon the researcher presenting an application that contains the following information:

      (1) Which Agency or organization is seeking the data;

      (2) Who the lead researcher or analyst will be;

      (3) The intended uses of the data;

      (4) An explanation as to how the Research is likely to bring benefits to the homeless service system, homeless service agencies involved, and/or directly to homeless persons;

      (5) The data elements desired, programs or components of the continuum of care to be included, and the time period covered;

      (6) A plan to provide for the security of the data in the course of the research;

      (7) A plan to provide for the return or proper disposal of all data at the conclusion of the research;

      (8) A plan to restrict additional uses or disclosures of the data (except where required by law); and

      (9) A statement of the applicant's willingness to sign a written agreement containing the foregoing elements.

   b. Conditions:

      (1) Partner Agencies will be notified if Agency identified specific data is being provided to researchers or other external parties.

      (2) Official requests for information will be handled strictly in compliance with relevant statutes and regulations. IHCDA administration will consult with the Data Collection and Evaluation Committee to acquire Stakeholder perspective.

      (3) IHCDA administration may approve data access but with modifications. That is, some changes may be made, for example, to the range of accessible data, the schedule for production of that data or who from the external party may have access to the data.

      (4) If IHCDA administration denies an external party access to the HMIS data or adds unacceptable modifications, that party may petition the IHCDA Executive Committee to review and possibly overturn the decision. The Executive Committee's decision shall be in its sole discretion and shall be final. The external party shall have no further right to appeal.

(5) If a researcher has obtained approval to conduct Research and later determines information is needed that differs from what was originally authorized, the Data Collection and Evaluation Committee approval process must be repeated.

c. The data elements the researcher requires will determine how they gain access to Protected Personal Information. If the elements needed meet the definition of Protected Personal Information, then the researcher has two options:

(1) Client Authorization from the Client or their legal representative: The authorization must contain certain elements in order to accommodate the request.

(2) Institutional Review Board (IRB) Waiver: A waiver of the Client authorization requirement is obtained from a recognized IRB.

If the information being requested is De-identified Information, then neither Client authorization, nor an IRB waiver is required; however, IHCDA administration approval shall still be required. It shall be the sole responsibility of the requesting researcher to obtain either Client authorization or an IRB waiver. It shall not be the responsibility of IHCDA or the Data Collection and Evaluation Board to obtain Client authorization or an IRB waiver.

2. Research Recruitment: Methods for obtaining Research subjects for a study must be approved in advance by the Data Collection and Evaluation Committee and will conform to legal and regulatory guidelines. When an approved study makes a change in their recruiting practice, the Data Collection and Evaluation Committee must re-approve the method before it is put into practice.

3. The Data Collection and Evaluation Committee Role: The Data Collection and Evaluation Committee is not a Privacy Board, nor is it an Institutional Review Board (IRB). The Data Collection and Evaluation Committee is responsible for:

a. Coordinating and monitoring Research activities that are conducted on the HMIS data. Any Research activity, regardless of funding source or original intent (*e.g.*, the activity may have started out as something else) is subject to Data Collection and Evaluation Committee oversight.

b. Providing an internal administrative feasibility review to assess: (a) the impact of Research on IHCDA staff, Partner Agencies or programs, IHCDA Clients; (b) the impact of Research outcomes, and (c) the quality of Research design if applicable. Research must be likely to bring benefits to the homeless service system, homeless service agencies involved, and/or directly to homeless people. The Data Collection and Evaluation Committee will make the final determination whether the Research request will be granted. The Data Collection and Evaluation Committee may from time to time adapt more specific criteria for evaluating Research requests.

c. Ensuring Client privacy rights are protected as it relates to Research or Research-related activities.

d. Maintaining documentation related to these activities in accordance with legal regulations, regardless of funding source or IRB approvals.

e. Clarifying activities (surveillance, program evaluation/quality improvement) that may contain elements of Research.

f. Referring cases of suspected misconduct to IHCDA Executive Committee.

g. Overseeing consent process for Research subjects who would be involved in on-going Research studies. It may be combined with an authorization. It must:

(1) Describe the study;

(2) Describe its anticipated outcomes and benefits;

(3) Describe how the confidentiality of records will be protected; and

(4) Notify the Client if photographs will be used and the purpose of the photographs.

4. Charges: Because there are costs in generating data files or reports, IHCDA administration may charge external parties for the costs occurred in generating the requested data. These costs will include but are not limited to: analyst time, printing costs, and computer time, among others. Applicable charges shall be in the sole discretion of IHCDA.

Data Integration and Legacy Data Migration

Policy:	IHCDA recognizes that some Agencies may want to keep their existing databases and import their data periodically into the HMIS. Further, Agencies may move legacy data into the HMIS from their existing databases. Data integration/migration is allowed, provided the data integrated is accurate and meets the format at technical specifications required by the HMIS Software Vendor. The Agency will be charged a fee for this service.

Procedure:

A. DATA INTEGRATION

Agencies who want to import data into the HMIS must enter into an HMIS Participation Agreement, meet all of the requirements stated in herein and other requirements established by IHCDA for the HMIS.

1. Agencies wishing to integrate data must contact IHCDA and describe the type of data, the amount of data proposed to be integrated, and the existing database that houses the data.

2. IHCDA will provide the Agency with an upload specification document for integration based on the Agency's request.

3. Agency shall review IHCDA's specification document and shall provide IHCDA with any supplemental information necessary based on the Agency's (and its vendors') capabilities.

4. Based on the foregoing, IHCDA shall provide Agency with an estimated cost for the integration.

5. Agency and IHCDA shall agree upon final implementation and costs.
6. All upload specifications must be met prior to the data integration.
7. Agencies will pay for the cost of any problems associated with the data integration at the standard rate charged by the HMIS Software Vendor.
8. Data that is integrated may be shared with other Agencies.

B. LEGACY DATA MIGRATION

1. Agencies wishing to migrate legacy data must contact the Indiana Planning Council on Homelessness and/or the CoC Board and describe the type of data, the amount of data to be moved, and the existing database that currently contains the data.
2. IHCDA will provide the Agency with an upload specification document for migration based on the Agency's request.
3. Agency shall review IHCDA's specification document and shall provide IHCDA with any supplemental information necessary based on the Agency's (and its vendors') capabilities.
4. Based on the foregoing, IHCDA will provide Agency with an estimated cost for the migration.
5. Agency and IHCDA must agree upon final implementation and costs.
6. All upload specifications must be met prior to the legacy data migration.
7. Agency will pay for the cost of any problems associated with the legacy data migration at the standard rate charged by the HMIS software vendor.
8. All legacy data that is migrated may not be shared with other Agencies without the consent of the Client(s) to whom the data relates.
9. Legacy data that is more than twelve (12) months old should not be migrated, unless the data is part of a program that has a length of stay that is generally longer than twelve (12) months.
10. The legacy data that is migrated must be accurate.